EXECUTIVE SUMMARY

An Overview of the State of External Attack Surface Management

2023 will be remembered for the magnitude of its technological advancements. The same can be said for the stealth and scale of its cybercriminal activity.

Attackers have adapted and continue to hone their techniques, as highlighted in this report. Our findings reveal that the number of targeted databases doubled from 2022 to 2023, and indicates a great deal of ingenuity.

Two significant attacks in 2023, along with the surrounding data, should serve as a wake-up call for your SOC team in 2024. These attacks demonstrate how cybercriminals consistently strike big and win even bigger.

1 The first explosive cyber incident affected **DarkBeam**, a London-based supply chain intelligence capability provider, which suffered a misconfiguration leading to the exposure of **3.8 billion sensitive records**.

2 The second cyber incident, the MOVEit breach, affected over **60 million individuals**, with **83.9% of primary victims**, companies in the United States. MOVEit, a company which provides secure managed file software, has impacted millions of businesses across sectors such as healthcare, supply chain and education. If we dig into this massive breach it follows a classic ransomware threat pattern, initiated via a zero-day vulnerability, and the Cl0p gang, a Russian-speaking ransomware gang, as the perpetrators. The U.S. Cybersecurity and Infrastructure Security Agency describes this group as "**driving global trends in criminal malware distribution**."

The evolution of ransomware threats becomes more intriguing. The Cl0p gang, which led the MOVEit attack, deployed their usual tactics of threatening to publish stolen sensitive data unless they received a ransom payment. This attack has cost nearly **$10 billion (USD)** and data in late 2023 shows that the Cl0p gang have earned an estimated **$100 million** for their efforts. Following the patterns of this one ransomware gang, we continue to see how their extortion tactics grow bigger and bolder. New notable victims that fell this year include Maximus, **an American government services company**, and Pôle emploi, the French government's unemployment agency.

What is more interesting in the evolution of ransomware threats is that the US government offered a **$10 million bounty** for information about the Cl0p gang post-attack. It highlights the sheer speed of cyberattacks.

Another notable breach in Pakistan reveals another edge to 2023 cyber data leaks. A breach of a restaurant database resulted in the compromise of **2.2 million Pakistani citizens' data**. This data was quickly put up for sale, highlighting how extensive cyber threats were across different domains and regions. No one industry can claim safety or an advantage against possible attacks.

These incidents underscore the critical importance of defending your external attack surface. They also emphasize the critical importance of robust cybersecurity measures to mitigate data exposure risks, emphasizing confidentiality, integrity, and availability principles to thwart adversaries and safeguard sensitive information. We will deep dive into this in our **Overview of the Attack Surface** section in this report, as we look at more context and data points.

Overall, CybelAngel's objective with the 2024 State of the External Attack Surface Report is twofold.

1 **We aim to shed light on the evolving threats that our clients, partners, and all cyber stakeholders face, as well as share data trends that consistently pose a security threat.**

2 **Finally, we encourage you to adopt a proactive cybersecurity approach that will allow you to avoid reactive policies and enhance your cyber defense in the event of an external attack surface breach.**

We hope that you will find this report a helpful guide for a more secure 2024.